7/6

DATE: ch 8

SUBJECT: Sec.4.

P.1

K = 5 ⇒ shifted by 5 letter يعني مشفر ~~[illegible]~~

P.2-

بيحرك لبعض الحروف فقط .

seven latter ALiseBo

261 ⇒ لو احنا مش عارفين

أي الـ sipher لأي حروف

واحنا معانا 7 حروف معروفة

$26 - 7 = 19$

$19!$

$26! - 19! \simeq 10^9$

P3

Yes هيقدر، وحتى لو مستخدم K

دونه يسهل عليه الفك .

P4

Block cipher.

T1 دونه ممكن تكون من Table الأصلي أو أي حاجه تانيه .

scrambler ⇒ بيلخبط جزء عليها Table

الداتا .

وتتكرر، مع loop دي أكتر من مرة "n Time" وكل ما n يتكبر كل ما

التشفير أفضل -

DATE :

SUBJECT :

(a) 1010 0000

T_1 ↓ _ _ 7 Times.

0000 0101

↘

0000 0101 ⌉ T_1
1010 0000 ⌋

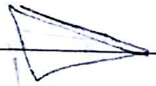
↘

1010 0000 ⌉ T_1
0000 0101 ⌋

↓ T_1

0000 0101 repeated 8 Time

(b) 1010 0000



1010 0001 ⌉ T_1
1000 0101 ⌋

↘

1000 0101 ⌉ T_2
1010 0001 ⌋

↘

1010 0001 ⌉ T_2
1000 0101 ⌋

1000 0101

repeat 7 time

DATE: SUBJECT:

C.a 1010 0000

↓

0000 0101   0000 0101

↓scan delar

1010 0000   1010 0000

1010 0000   1010 0000

0000 0101   0000 0101

↓SC   ↓sar

1010 0000   1010 0000

1010 0000   1010 0000

0000 0101   0000 0101

↓   ↓

1010 0000   1010 0000

C.b.

1010 0000   1010 0001

0000 0101   1000 0101

1010 0001   7Times   1010 000

1010 0001   1010 0000

1000 0101   0000 0101

1010 0000   1010 0001

1010 0000   1010 0001

0000 0101   1000 0101

1010 0001 →   7Times   ← 1010 000

DATE:

SUBJECT: 4 3

P.6 100 100 1000

011 011 011

Sniffs

hack عالداتا ويسمع الداتا.

هتفهمها لما تشوف patern من 3bit مكرر ٣مرات.

IV = 111 → C(0)

$m = 100\ 100\ 1000$ — $m(1) = 100$, $m(2) = 100$, $m(3) = 100$

$C_i = K_s(m_i \oplus C_{(i-1)})$

$C_1 = K_s(m(1) \oplus C(0)) = K_s(100 \oplus 111)$

$= K_s(011) = 100$

$= 1$

صح الرد

$C_2 = K_s(m(2) \oplus C_1) = K_s(100 \oplus 011) = K_s(0\ 00) = 110$

$C_3 = K_s(m(3) \oplus C_2 = K_s(100 \oplus 110) = K(010) = 101$

$m = 100\ 100\ 1000$

$100\ 110\ 101$

P.7 RSA " public, private Keys " هاص موضوع "

P.9 لفضيل كوينو آلياء
لكن العمليات هتكون أصعب،

① بنختار رقم لـ p, q

$p=3 \quad q=11$

$n = pq = 33$

$z = (P-1)(q-1) = 2 \times 10 = 20$

2- $(e < n)$ has no common factors with Z

$Z = 20 \quad 10 \quad 5 \; 4 \quad 2 \quad 1$

- $e = 9$
- $d \Rightarrow ed \% Z = 1 \qquad d = 9$

$9d \% 20 = 1 \Rightarrow 81 / 20 = 1$

Public Key (n, e)

private Key (n, d)] → , دول اللي بيستخدموا في incryption decryption.

ⓐ

$\begin{pmatrix} d & o & g \\ 4 & 15 & 7 \end{pmatrix}$

incryption

d $(m = 4 \quad C = m^e \% n)$

$(m = 4 \quad = 4^9 \% 33)$

o $(m = 15 \quad C = 15^9 \% 33 =)$

g $(m = 7 \quad C = 7^9 \% 33 =$

decryption

$m = C^9 \% n \qquad = 4$

ⓑ dog

4 15 7 → [هنحول كل واحد منهم binary [illegible]]

26 5 bite.

$\underbrace{(00100}\,\underbrace{01111}\,\underbrace{00111)}_2$

DATE : ______ SUBJECT : ______

• لازم نحول binary ← decimal و نس dest

يعرف قيم الداتا الفعلية 5bits binary ← decimal ب

P, g

$T_A = g^{S_A} \% P$ $T_B = g^{S_B} \% P$

lise. $S = T_B^{S_A} \% P$ BoB $S' = T_A^{S_B} \% P$

(S. 712 P. 685

قانون

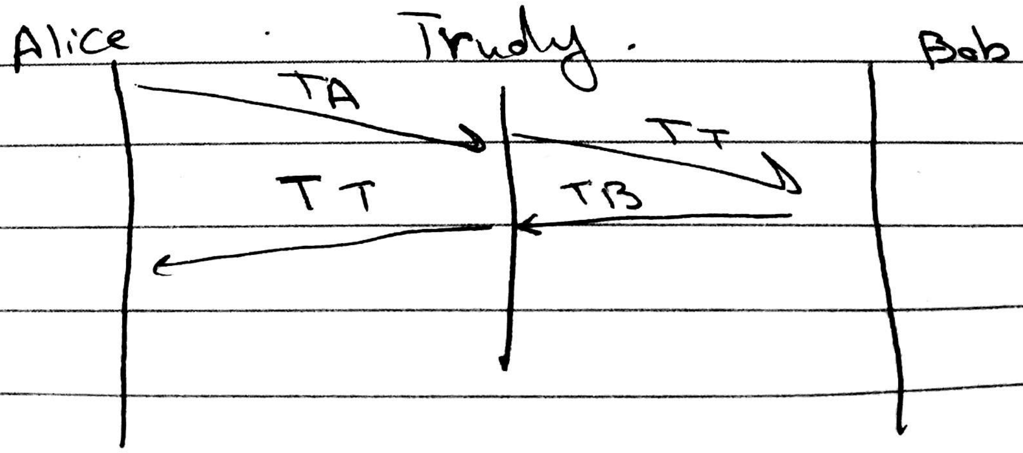
$(a \bmod n)^d \bmod n = a^d \bmod n.$

$S = T_B^{S_A} \% P - [g^{S_B} \% p]^{S_A} \% P$

$= \cancel{T_B^{S_A} \% P} \to [g^{S_B \cdot S_A} \% P] \% P$

$\cancel{T_B^{S_A} \% P} \to \underline{[g^{S_A} \% P]}^{S_B} \% P$

$= T_A^{S_B} \% P = S'$ ※



(1)

Con
sheet 8

Security.

see

Authentication → (PKI) public Key incryption.

Integrety → hash . وصول الرسالة مظبوطه

send m → H(m) $\xrightarrow{\text{يبعت}}$ H(m) + m.

rcvd ↳ H( ) + m → H(m) → لو ساوت = مظبوطه

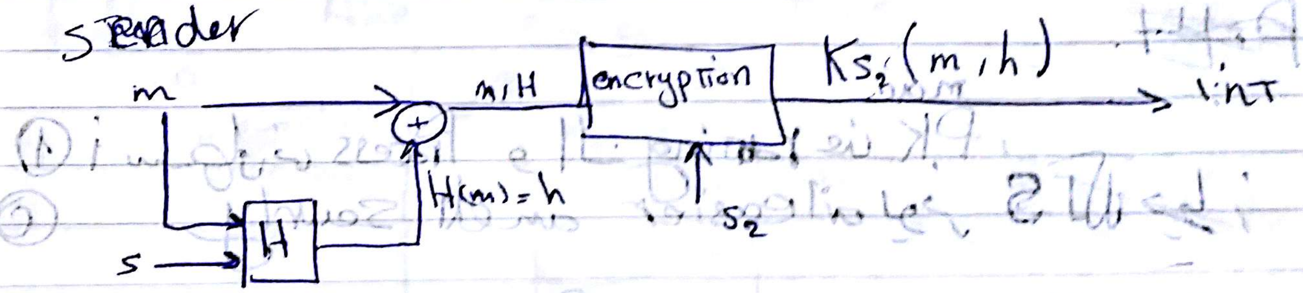
P.H Fig 8.8) (7.17)

مش هينفع

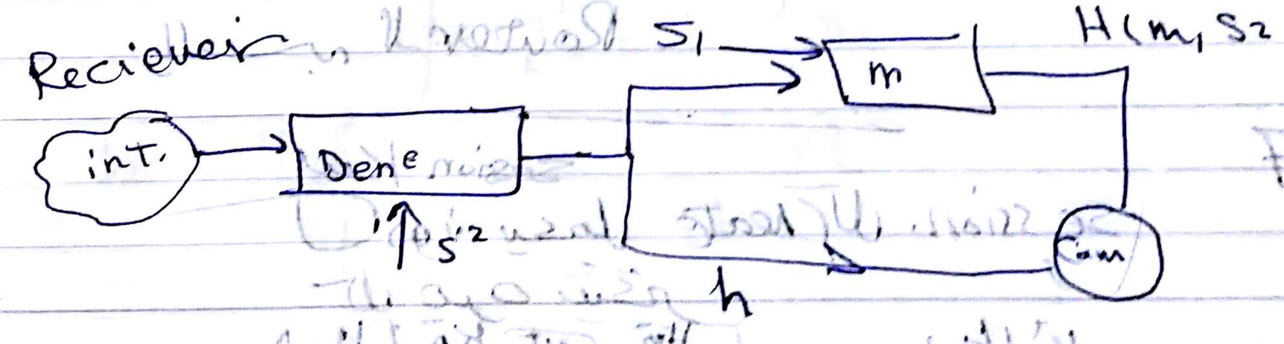
الـ H بيطلع نفس H(m) لرسايل مختلفين

P.12 Fig(7.19)

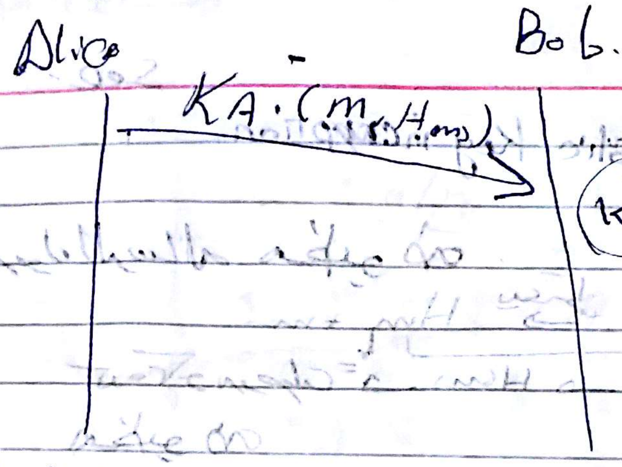
S~~Reader~~der



Reciever



P.14.



لو integrety

$K_A^+ (K_A^- (m, H)) = m, H$

public Key

authentication

و ويعرفه منا Alice

Certificate يعرفه KA بتاع كل الرعايا الثقة

authority (C.A)

مش بنات كلام الرسالة

بيفكرها الـ PK بتاع الموقع

انه بتاعه لو مش هو هيعرف

ان الرسالة اتسرقت

~~P.14~~

mac

① i سهل تبني Process والـ routing PK,

© security and easier ال يوفر S كل مرة،

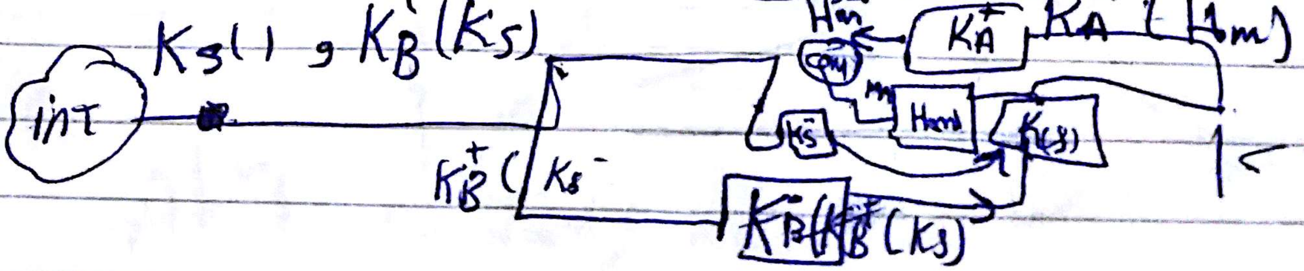
بالنسبة للRouter

P.17

Session Key

ذوي بيعمل Create للsession.

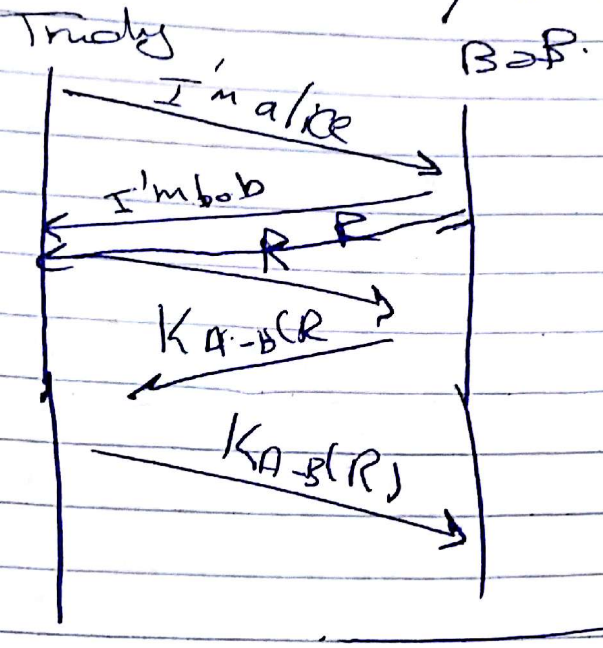
كل مرة بيتكرر



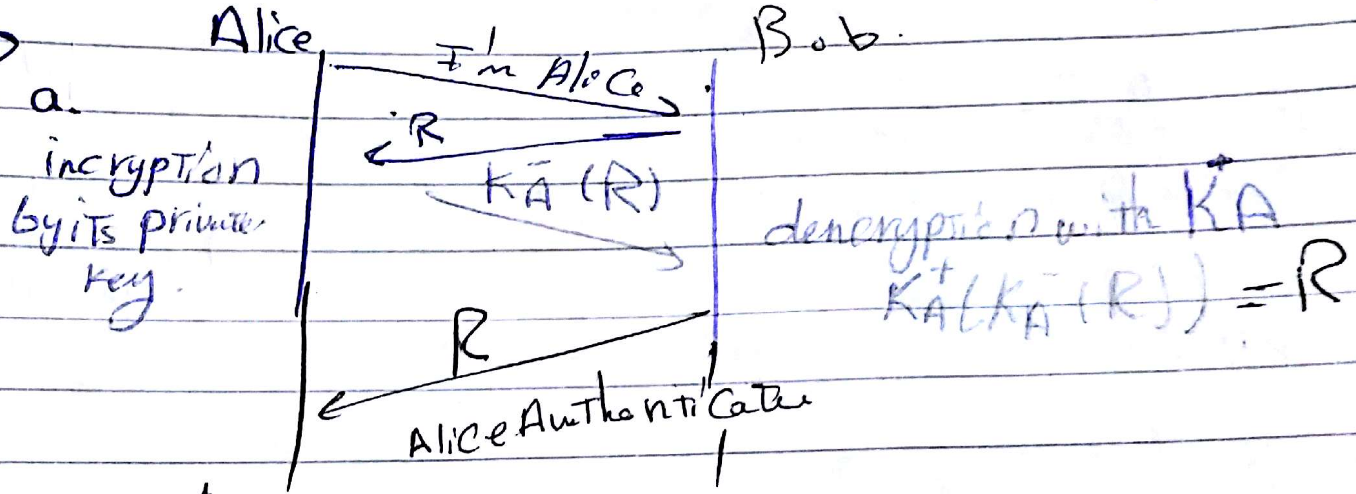
P.15

nonce →

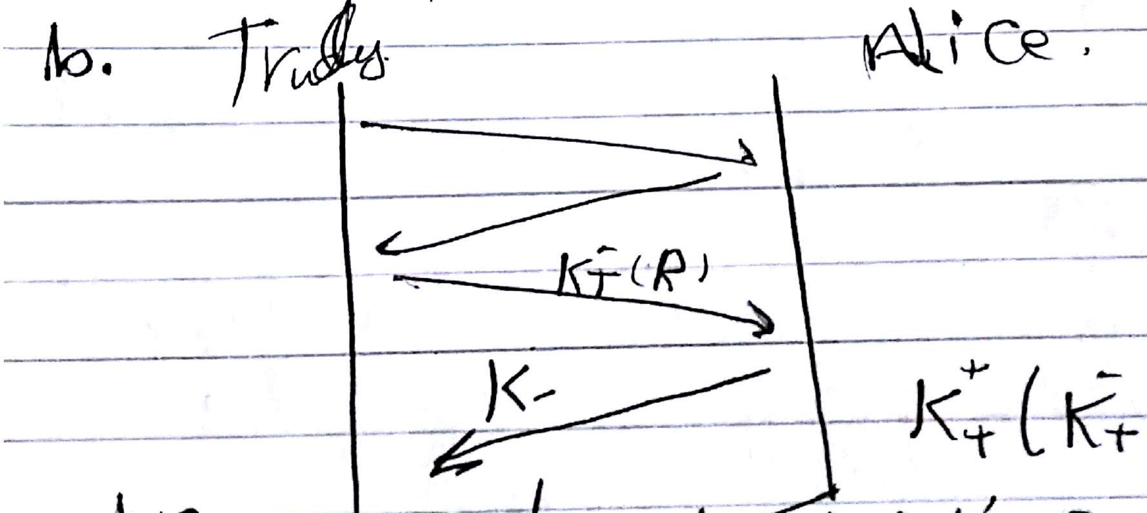
انم بيستخدم لمرة واحدة



P.16



b.



وهنا هيفتكر انه Trudy هو Alice